DOCTORAL THESIS

Biometric system security and privacy: data reconstruction and template protection

Mai, Guangcan

Date of Award:
2018

Abstract

Biometric systems are seeing increasing use, from daily entertainment to critical applications such as security access and identity management. Biometric systems should thus meet the stringent requirement of a low error rate. In addition, for critical applications, biometric systems must address security and privacy issues. Otherwise, severe consequences may result, such as unauthorized access (security) or the exposure of identity-related information (privacy). It is therefore imperative to study vulnerability to potential attacks and identify the corresponding risks. Furthermore, countermeasures should be devised and patched on the systems.

In this thesis, we study security and privacy issues in biometric systems. We first attempt to reconstruct raw biometric data from biometric templates and demonstrate the security and privacy issues caused by data reconstruction. We then make two attempts to protect biometric templates from reconstruction and improve the state-of-the-art biometric template protection techniques.

To summarize, this thesis makes the following contributions.

- **Data Reconstruction**: An investigation of the invertibility of face templates generated by deep networks. To the best of our knowledge, this is the first such study of the security and privacy of face recognition systems.
- **Template Protection**: An end-to-end method for simultaneous extraction and

protection of templates given raw biometric data (e.g., face images). To the best of our knowledge, this is the first end-to-end method for the direct generation of secure templates from raw biometric data.

- **Template Protection**: A binary fusion approach for multi-biometric cryptosystems to offer accurate and secure recognition. The proposed fusion approach can simultaneously maximize the discriminability and entropy of the fused binary output.

Keywords: biometric template, biometric security, data reconstruction, template reconstruction, and template protection

Table of Contents